



CÓDIGO: MAGI-01

VERSIÓN: 03

FECHA: 27/11/2024

MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.

CUADRO CONTROL DE CAMBIOS		
Versión	Fecha	Descripción del Cambio
00	02/06/2021	Emisión inicial
01	10/06/2021	Cambio de nombre por Manual de Administración de Tecnología, Seguridad y Privacidad de la Información
02	14/10/2022	Actualización general del Manual de Administración de Tecnología, Seguridad y Privacidad de la Información 2022
03	27/11/2024	Actualización completa del Manual de Administración de Tecnología, Seguridad y Privacidad de la Información 2024

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 2 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

TABLA DE CONTENIDO

1. INTRODUCCION	4
2. CONCEPTOS FUNDAMENTALES	5
3. OBJETIVO GENERAL	7
4. OBJETIVOS ESPECIFICOS.....	7
5. ALCANCE.....	8
6. AUTORIDAD Y RESPONSABILIDAD	8
6.1. COMPROMISOS DE LA GERENCIA	9
6.2. RESPONSABILIDAD	9
6.3. CUMPLIMIENTO Y VIOLACIONES.....	9
6.4. APROBACIÓN Y ACTUALIZACIÓN DE LAS POLÍTICAS	12
6.5. VIGENCIA DEL DOCUMENTO	12
7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	13
7.1. ORGANIZACIÓN INTERNA	13
7.1.1. Roles y Responsabilidades Para la Seguridad de la Información	13
8. DISPOSITIVOS MOVILES Y TELETRABAJO	14
8.1. POLÍTICAS PARA DISPOSITIVOS MÓVILES.....	14
8.2. TRABAJO EN CASA Y ACCESO REMOTO	14
9. SEGURIDAD EN EL RECURSO HUMANO	17
10. GESTION DE ACTIVOS DE INFORMACIÓN	17
10.1. RESPONSABILIDAD POR LOS ACTIVOS DE INFORMACIÓN	17
10.1.1. Inventario de Activos de Información	17
10.1.2. Propiedad de los Activos de información	18
10.1.3. Uso aceptable de Activos	19
10.2. CLASIFICACIÓN DE LA INFORMACIÓN	24
10.2.1. Clasificación de la Información	24

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 3 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

10.3.	MANEJO DE MEDIOS.....	24
10.3.1.	Gestión de Medios Removibles	24
11.	CONTROL DE ACCESO.....	25
11.1.	REQUISITOS DE EMPAS PARA EL CONTROL DE ACCESO.....	25
11.1.1.	Política de Control de Acceso Lógico.....	26
11.1.2.	Acceso a Redes y Servicios de Red	27
11.2.	GESTION DE ACCESO DE USUARIOS	32
11.3.	RESPONSABILIDAD DE LOS USUARIOS.....	35
11.4.	CONTROL DE ACCESO A LOS SISTEMAS Y APLICATIVOS.....	36
12.	SEGURIDAD FISICA Y DEL ENTORNO.....	37
12.1.	ÁREAS SEGURAS.....	37
12.2.	EQUIPOS	38
13.	SEGURIDAD DE LAS OPERACIONES.....	41
13.1.	PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES.....	41
13.2.	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	41
13.3.	COPIAS DE RESPALDO	44
13.4.	REGISTRO Y SEGUIMIENTO	45
13.5.	CONTROL DE SOFTWARE OPERACIONAL.....	46
13.6.	GESTIÓN DE LA VULNERABILIDAD TÉCNICA.....	47
14.	SEGURIDAD DE LAS COMUNICACIONES.....	48
14.1.	GESTIÓN DE LA SEGURIDAD DE LAS REDES.....	48
14.2.	TRANSFERENCIA DE INFORMACION.....	50
15.	REFERENCIAS	50
	ANEXOS	51

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 4 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

1. INTRODUCCION

La información es un recurso valioso para la Empresa, comparable en importancia a otros activos cruciales. Por lo tanto, debe ser protegida adecuadamente para asegurar la continuidad de los sistemas de información, minimizar los riesgos de daño y contribuir a una gestión eficaz.

Para que los principios de seguridad de la información sean efectivos, es esencial implementar políticas que formen parte integral de la cultura organizacional de la Empresa. Esto requiere el compromiso de todos los empleados vinculados a la gestión de la información, para promover la difusión, consolidación y cumplimiento de estas políticas.

La Seguridad Informática implica evaluar y gestionar los riesgos basándose en políticas y estándares diseñados para satisfacer las necesidades específicas de la Empresa. La Administración General de EMPAS S.A. proporciona a directivos, funcionarios, empleados y trabajadores las herramientas técnicas e informáticas necesarias para asegurar la eficacia y rapidez en la prestación de servicios. Esto incluye equipos, programas, sistemas, acceso a redes internas y externas, así como el uso de correo electrónico y teléfonos.

Los sistemas de información deben facilitar y agilizar los procedimientos administrativos, operativos, comerciales y de proyectos, asegurando la disponibilidad, autenticidad, confidencialidad e integridad de la información para una toma de decisiones informada y el buen funcionamiento de la Empresa. El uso de estos sistemas debe ser una norma general para todos los miembros de EMPAS S.A., y no dejarse al criterio individual de los usuarios.

La creciente conectividad ha aumentado la exposición de los sistemas de información y las redes a un número creciente de amenazas, lo que presenta nuevos retos en el ámbito de la seguridad. Esto subraya la necesidad de una mayor conciencia sobre los aspectos de seguridad y el desarrollo de una "cultura de seguridad".

		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 5 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

En cumplimiento con las competencias de la Gerencia General sobre la administración de los bienes tangibles e intangibles de la Empresa, este documento establece las Políticas y Estándares de Seguridad de la Información.

2. CONCEPTOS FUNDAMENTALES

- **Activos de información:** elementos de hardware y software que permiten la administración y funcionamiento de la información.
- **Autenticación:** Es la propiedad que me permite identificar el generador de la información. Por ejemplo, al recibir un mensaje de alguien, estar seguro que es de ese alguien el que lo ha mandado, y no una tercera persona haciéndose pasar por la otra (suplantación de identidad). En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso.
- **Clasificación de la información:** ejercicio en la que se determina el nivel de importancia de la información que se maneja en una entidad asegurándola y garantizándole una adecuada administración.
- **Confidencialidad:** Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados. Así mismo, la confidencialidad es el acceso a la información únicamente por personas que cuenten con la debida autorización
- **Custodio técnico:** proceso o grupo de trabajo encargado de administrar y hacer efectivo los controles de seguridad de la información disponibles en la entidad.
- **Disponibilidad:** Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Así mismo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.
- **Dominios de control:** guía que permite garantizar la seguridad de la información.
- **Help Desk:** Soporte técnico brindado a los usuarios telefónicamente, su función es proveer conocimientos especializados de los sistemas de producción para

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 6 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

identificar y asistir en el ámbito / desarrollo de sistemas y en la resolución de problemas.

- **Información:** Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro
- **Integridad:** Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) Así mismo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.
- **Legalidad:** Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
- **Propietario de la información:** designación de un propietario o grupos que tienen la responsabilidad de definir quienes tienen acceso a la información y que se debe hacer con esta.
- **Responsable de Seguridad Informática:** Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran
- **Seguridad de la información:** Conjunto de políticas de uso y medidas que afectan al tratamiento de los datos que se utilizan en una organización.
- **Sistema de Información:** Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.
- **Tecnología de la Información:** Se refiere al hardware y software operados por la Empresa o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la Empresa, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.
- **Usuario:** Cualquier persona que genere, obtenga, transforme, conserve o utilice información de la Entidad en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la compañía.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 7 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- **VPN:** por sus siglas en inglés: Virtual Private Network es una tecnología que permite a las organizaciones crear una conexión segura y cifrada a través de una red pública, como Internet, para acceder a sus recursos internos de forma segura.
- **Webmail:** es un servicio de correo electrónico accesible a través de un navegador web, en lugar de utilizar un cliente de correo electrónico instalado en un dispositivo. Permite a los usuarios enviar, recibir y gestionar sus correos electrónicos desde cualquier lugar con acceso a Internet, sin necesidad de software específico para correo.

3. OBJETIVO GENERAL

Establecer directrices y lineamientos para la gestión de seguridad y privacidad de la información en la Empresa Pública de Alcantarillado de Santander S.A. E.S.P.

4. OBJETIVOS ESPECIFICOS

1. Proteger los recursos de información de EMPAS S.A y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y legalidad de la información.
2. Asegurar la implementación efectiva de las medidas de seguridad descritas en esta Política de Seguridad de la Información, mediante la identificación y asignación de los recursos necesarios y la provisión de las partidas presupuestales correspondientes.
3. Fomentar una cultura de seguridad de la información mediante la socialización de las políticas de seguridad a todos los usuarios, asegurando que comprendan su importancia y adopten prácticas adecuadas para proteger los sistemas de información.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 8 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

4. Incrementar la concientización sobre el riesgo de no dar uso adecuado a los sistemas de información, así como la necesidad de adoptarlos e implementarlos.
5. Establecer controles precisos que determinen la mayor eficiencia en la seguridad de los sistemas de información de EMPAS S.A, evitando aquellas prácticas que supongan la utilización incorrecta o inadecuada de los sistemas de información.
6. Comprometer a todos los Usuarios de las Tecnologías de la Información a implementar principios básicos como conciencia y responsabilidad sobre la seguridad y manejo de la información.

5. ALCANCE

El presente manual consigna todas las políticas de gestión de seguridad y privacidad de la información de EMPAS S.A, para salvaguardar todos los activos de información y que son de obligatorio cumplimiento por parte de los servidores públicos, contratistas, proveedores y funcionarios.

Se establecen las Políticas y Estándares de Seguridad de la Información, teniendo en cuenta que cada usuario es un actor importante para garantizar la seguridad, por lo que cada uno, de acuerdo a las funciones que desempeña, deberá estar consciente de los riesgos y de las medidas preventivas pertinentes, deberá asumir la responsabilidad correspondiente y tomar las medidas que permitan fortalecer la seguridad de los sistemas de información

6. AUTORIDAD Y RESPONSABILIDAD

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 9 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

6.1. COMPROMISOS DE LA GERENCIA

La gerencia de la Empresa Pública de Alcantarillado de Santander apoya de manera activa el establecimiento, mantenimiento y mejora continua de las políticas de seguridad de la información que se implementan en la entidad, a través de:

- Revisiones periódicas a las políticas de seguridad y privacidad de la información, así como el cumplimiento de estas.
- Asignación de recursos para gestión de la seguridad de la información.
- Promover la importancia de la seguridad de la información en la entidad para que los funcionarios de EMPAS obtengan una cultura organizacional de la seguridad y privacidad de la información.
- Apoyar el cumplimiento del Modelo de Seguridad y Privacidad de la Información definido por el MINTIC, las normas y estándares que lo complementen.

6.2. RESPONSABILIDAD

Es responsabilidad de la gerencia, subgerentes, asesores y jefes de oficina de la Empresa Pública de Alcantarillado de Santander hacer uso de las políticas de seguridad y privacidad de la información, como parte de sus herramientas de su gestión.

6.3. CUMPLIMIENTO Y VIOLACIONES

El cumplimiento de la política de seguridad y privacidad de la información se aplican a todos los servidores públicos, contratistas, proveedores y funcionarios que interactúan con los activos de información de la empresa o en calidad de responsables, custodio o usuarios. En el caso de que se constate alguna violación de las normas establecidas por la presente política de seguridad, se aplicará lo dispuesto en la ley 734 de 2002, por el incumplimiento de los Deberes contenidos en el Art. 34 numerales 1, 2, 4, 5, 7, 11, 21, 22, 24 y 25, Ley 1273 de 2009 Delitos Informáticos y la Ley 1581 de 2012 de Protección de Datos Art. 23 y 24.

DEBERES (Artículo 34 Ley 734 de 2002). Son deberes de todo servidor público:

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 10 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

1. Cumplir y hacer que se cumplan los deberes contenidos en la Constitución, los tratados de Derecho Internacional Humanitario, los demás ratificados por el Congreso, las leyes, los decretos, las ordenanzas, los acuerdos distritales y municipales, los estatutos de la entidad, los reglamentos y los manuales de funciones, las decisiones judiciales y disciplinarias, las convenciones colectivas, los contratos de trabajo y las órdenes superiores emitidas por funcionario competente. Los deberes consignados en la Ley 190 de 1995 se integrarán a este código.
2. Cumplir con diligencia, eficiencia e imparcialidad el servicio que le sea encomendado y abstenerse de cualquier acto u omisión que cause la suspensión o perturbación injustificada de un servicio esencial, o que implique abuso indebido del cargo o función.
4. Utilizar los bienes y recursos asignados para el desempeño de su empleo, cargo o función, las facultades que le sean atribuidas, o la información reservada a que tenga acceso por razón de su función, en forma exclusiva para los fines a que están afectos.
5. Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o función conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebidos.
7. Cumplir las disposiciones que sus superiores jerárquicos adopten en ejercicio de sus atribuciones, siempre que no sean contrarias a la Constitución Nacional y a las leyes vigentes, y atender los requerimientos y citaciones de las autoridades competentes.
11. Dedicar la totalidad del tiempo reglamentario de trabajo al desempeño de las funciones encomendadas, salvo las excepciones legales.
21. Vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente, de conformidad con los fines a que han sido destinados.
22. Responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización.
24. Denunciar los delitos, contravenciones y faltas disciplinarias de los cuales tuviere conocimiento, salvo las excepciones de ley.

		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 11 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

25. Poner en conocimiento del superior los hechos que puedan perjudicar el funcionamiento de la administración y proponer las iniciativas que estime útiles para el mejoramiento del servicio.

LEY 1273 DE 2009 DE DELITOS INFORMÁTICOS EN COLOMBIA

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

A continuación, se mencionan los artículos que componen esta ley:

- Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO
- Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.
- Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS
- Artículo 269D: DAÑO INFORMÁTICO
- Artículo 269E: USO DE SOFTWARE MALICIOSO
- Artículo 269F: VIOLACIÓN DE DATOS PERSONALES
- Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES
- Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 12 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS

Ley 527 de 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se dictan otras disposiciones.

Ley 1712 de 2014 Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Ley 1952 de 2019 Por medio de la cual se expide el Código General Disciplinario, se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario.

Decreto Nacional 1377 de 2013 Por el cual se reglamenta parcialmente la Ley 1581 de 2012.

Decreto Nacional 103 de 2015 Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.

Decreto MinTIC 1008 de 2018 Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

6.4. APROBACIÓN Y ACTUALIZACIÓN DE LAS POLÍTICAS

Toda política de seguridad y privacidad de la información nueva, actualizada, y/o eliminada, será propuesta por el Área de Sistemas de Información y aprobada por el grupo de trabajo de arquitectura empresarial estas políticas serán revisadas como mínimo una vez al año y/o cada vez que surjan cambios sustanciales o sean requeridos.

6.5. VIGENCIA DEL DOCUMENTO

Las políticas contenidas en este documento estarán vigentes desde la fecha de su aprobación y divulgación.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 13 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

7.1. ORGANIZACIÓN INTERNA

7.1.1. Roles y Responsabilidades Para la Seguridad de la Información

Todos los funcionarios públicos, contratistas y terceros de EMPAS, deben conocer y cumplir el modelo de seguridad y privacidad de la información establecido en la empresa; la gestión de la seguridad y privacidad de la información incluye a todos los niveles organizacionales de la entidad, por lo que se asignan roles y responsabilidades para el cumplimiento de las políticas de seguridad y privacidad de la información.

I. Nivel Estratégico

Rol Comité Arquitectura Empresarial: asume la responsabilidad entorno a la planeación, ejecución, cumplimiento y mejora continua de las políticas de seguridad y privacidad de la información de EMPAS.

II. Nivel Operacional

Teniendo en cuenta que la Subgerencia de Planeación e Informática está integrado en este comité y ejerce la secretaria técnica, tiene la responsabilidad con el equipo interdisciplinario del Área de Sistemas de Información de garantizar el cumplimiento de las Políticas de Seguridad y privacidad de la información.

III. Nivel Comunidad

Todos los servidores públicos, contratistas y proveedores que pertenecen a EMPAS deben conocer y cumplir con las políticas de seguridad y privacidad de la información, salvaguardar los principios de seguridad de los activos de información, asistir a las capacitaciones y sensibilizaciones que programe la entidad en temas de seguridad de la información, aplicación y cumplimiento de controles para la protección de la información, identificación y clasificación de activos de información junto con un análisis de riesgo.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 14 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

8. DISPOSITIVOS MÓVILES Y TELETRABAJO

8.1. POLÍTICAS PARA DISPOSITIVOS MÓVILES

EMPAS S.A. debe controlar la seguridad de la información cuando se usan medios de computación móvil; para salvaguardar la información se debe:

- Estar autorizado para que los dispositivos móviles interactúen con la infraestructura para el procesamiento de la información de EMPAS S.A.
- Las personas autorizadas para el uso de dispositivos móviles que requiera tener acceso a la información desde redes externas podrán acceder remotamente mediante un proceso de autenticación.
- Concientizar a los funcionarios y contratistas sobre el riesgo de usarlos dispositivos móviles para manejar los sistemas de información como para la infraestructura tecnológica de la entidad.
- La información y los equipos de EMPAS S.A. E.S.P. que se utilizan fuera de la oficina siguen siendo propiedad de la empresa. Estos equipos están destinados exclusivamente para tareas autorizadas por la empresa y no para usos personales. La información y los equipos que se extraen de la oficina deben ser protegidos por los colaboradores con el mismo nivel de cuidado que se les brinda dentro de las instalaciones de la empresa.
- Los equipos portátiles, tablets, teléfonos móviles y sus accesorios son especialmente susceptibles a robo o pérdida y requieren unas medidas de seguridad más altas. En ningún momento se deben dejar descuidados en sitios públicos.

8.2. TRABAJO EN CASA Y ACCESO REMOTO

Es importante definir y conocer las diferencias entre trabajo en casa y acceso remoto el primero se refiere a un modelo laboral donde los empleados trabajan desde su hogar de forma **permanente o regular**, sin necesidad de presentarse en la oficina y el acceso remoto corresponde a la necesidad de acceder a los recursos de la red corporativa desde **cualquier ubicación externa**, pero no implica un modelo laboral permanente o regular.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 15 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

La modalidad de trabajo en casa será posible para el personal vinculado a la empresa. Únicamente se asignarán conexiones a la red de EMPAS S.A. para trabajo en casa cuando sea solicitado por escrito por el área de Gestión Humana quien evaluará los casos y dará la viabilidad al área de Sistemas de Información, estableciendo las condiciones en tiempo (fecha inicio y fecha de finalización del trabajo en casa), indicando si el tipo de conexión es a través de VPN (permitiendo el acceso a los aplicativos de uso institucional - intranet) o un cliente de escritorio remoto (acceso local a la máquina del usuario).

El área de sistemas de información se encargará de implementar los controles de seguridad físicos y tecnológicos para proteger la confidencialidad, integridad y disponibilidad de la información y socializar las medidas de seguridad y privacidad, las buenas prácticas para proteger la misma. Los funcionarios que tengan conexión remota, no deben instalar ningún software en los equipos designados por la entidad.

Acceso Remoto

El acceso remoto a través de VPN debe ser autorizado únicamente para empleados y contratistas que lo necesiten por razones justificadas, como trabajo remoto, restricciones médicas, desplazamientos o proyectos específicos.

La solicitud de acceso debe pasar por un proceso formal de autorización, validado por el asesor de gestión humana (en casos de recomendaciones o restricciones medicas) o el jefe inmediato del área (asesor y subgerente) para los demás casos: (trabajo remoto, desplazamientos a otros sitios fuera de la empresa), quien aprobará y autorizará la petición y este a su vez la reenviará al área de sistemas través del correo ayuda@empas.gov.co quién será la encargada de asignar las conexiones remotas.

Bajo ninguna circunstancia se debe compartir el acceso o las credenciales de VPN con terceros o compañeros de trabajo.

El acceso remoto debe realizarse desde dispositivos que cumplan con las políticas de seguridad de la empresa, como el uso de antivirus y sistemas operativos actualizados.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 16 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

Los usuarios son responsables de garantizar que sus dispositivos estén protegidos contra malware, accesos no autorizados y otras amenazas que puedan poner en riesgo la red empresarial, no se permite descargar, instalar o ejecutar software no autorizado que pueda comprometer la seguridad de la red o violar las políticas de propiedad intelectual, el usuario es responsable de la legalidad del software instalado.

Los usuarios deben reportar de inmediato cualquier incidente de seguridad o anomalía detectada en el uso del acceso remoto.

El procedimiento para estos accesos es el siguiente:

- a. El funcionario que requiera la conexión por VPN o acceso remoto, debe hacer la solicitud de través de su jefe de área, a través de un correo al área de sistemas, una vez recibido el correo, el asesor de sistemas se comunica con el gerente para la autorización de dicha VPN o acceso remoto.
- b. Si la solicitud es aprobada, el área de sistemas asigna un numero de VPN y una contraseña de acceso al funcionario en el Firewall y se lleva una relación en una bitácora.
- c. Se procede a contactar al funcionario para realizar la respectiva configuración en el pc de su propiedad. Esta conexión VPN solo está habilitada para ingresar a la intranet e interactuar con los diferentes aplicativos.
- d. Si la conexión remota es autorizada, igualmente se realiza la configuración respectiva y se capacita al funcionario con respecto a la forma de establecer la conexión (conectar la VPN), además se le informa que el pc asignado en la empresa debe permanecer encendido y reiniciarlo, las veces que sea necesario (previo aviso del área de sistemas) para evitar bloqueos y permitir actualizaciones propias del sistema. Esta conexión remota permite al usuario trabajar con los documentos, archivos de su escritorio y correo Outlook como si estuviera ubicado frente al pc en la empresa.
- e. Si la modalidad aprobada es la de trabajo en casa, el funcionario aporta el pc personal.
- f. Cuando se requiere la modalidad de teletrabajo, este debe ser autorizado por el jefe inmediato y la gerencia. Se debe solicitar el permiso a servicios Generales para la salida del equipo de cómputo de las instalaciones de EMPAS a la residencia del funcionario.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 17 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

9. SEGURIDAD EN EL RECURSO HUMANO

Todo el personal adscrito a la empresa, debe presentar al área de Sistemas de Información el formato **FOGI-04 Registro de Autorizaciones** disponible en la intranet a través del repositorio Visión Calidad debidamente diligenciado, para la creación de cuenta de usuario de dominio, correo institucional, privilegio de navegación en internet, puertos USB, escritura en unidad DVD y autorización de roles y permisos de acuerdo a su perfil en los aplicativos institucionales; cuando el personal de planta es asignado a una nueva dependencia se hace necesario diligenciar nuevamente dicho formato con la asignación de los nuevos roles en los aplicativos acorde a las funciones asignadas por el jefe o consignadas en el manual de funciones propias del cargo; una vez finalice la relación laboral con la empresa, el exfuncionario debe presentar el formato de paz y salvo FOGH-19 debidamente diligenciado, luego se procederá a revocar el acceso y restablecer las contraseñas de todas las aplicaciones (aplicaciones, dominio, VPN, correo corporativo)

Para el caso de los contratistas la autorización de acceso y perfiles tendrán vigencia hasta la fecha de caducidad del contrato, la cual debe ser diligenciada en el formato, una vez finalice el contrato se deberá presentar diligenciada la certificación de paz y salvo (Prestación de Servicios Profesionales o Personales y Practicantes EMPAS S.A. FOGCO-90).

10. GESTION DE ACTIVOS DE INFORMACIÓN

EMPAS S.A. cuenta con una metodología, procedimiento, guía y formatos para identificar, clasificar y valorar los activos de información de todos los procesos al interior de la Entidad.

10.1. RESPONSABILIDAD POR LOS ACTIVOS DE INFORMACIÓN

10.1.1. Inventario de Activos de Información

El inventario de los activos de información se hace con la finalidad de identificar, clasificar y evaluar todos los activos de información críticos dentro de la empresa. Esto incluye hardware, aplicaciones y otros recursos relacionados con la gestión de

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 18 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

información. El inventario busca asegurar que todos los activos sean reconocidos y gestionados adecuadamente, facilitando la protección de la información, la evaluación de riesgos y la implementación de medidas de seguridad efectivas. Además, proporciona una base sólida para la toma de decisiones sobre la asignación de recursos, el cumplimiento de normativas y la planificación de la continuidad del negocio.

- Toda la información en reposo (almacenamiento), en tránsito (movimiento) o en uso (procesamiento) que utiliza los recursos físicos y tecnológicos de EMPAS S.A. es de propiedad de la empresa, a menos que se especifique lo contrario a través de un contrato u otro medio legal suscrito por el Representante legal de la empresa. Por ello, el tratamiento de la información institucional está sujeto a lo establecido en las cláusulas de propiedad intelectual y confidencialidad incluidas en los contratos establecidos con los funcionarios y en los contenidos de este manual, con objeto de garantizar que no se realice uso de esta, con propósitos personales comerciales o de otra índole.
- EMPAS S.A. E.S.P. dispone de una infraestructura tecnológica propia para el almacenamiento dedicado de los activos de información al servicio de los funcionarios y entes de control que requieren tener acceso a la misma garantizando la disponibilidad, integridad y confidencialidad de los datos, y facilitando el acceso controlado a los usuarios según sus permisos y necesidades.
- Todos los funcionarios, contratistas y terceros deben hacer entrega de los activos de información que se encuentran bajo su custodia al terminar su contrato y/o cada vez que el mismo haga cambio de dependencia o responsabilidades al interior de EMPAS S.A.

10.1.2. Propiedad de los Activos de información

EMPAS S.A. E.S.P. conservará siempre los derechos legales y la propiedad de los activos de información y el usuario o dependencia que haga uso de dichos activos será la responsable de mantener la calidad, integridad y disponibilidad del activo,

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 19 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

así como de cumplir con las políticas de protección de datos personales y regulaciones pertinentes.

El uso del activo de información se le debe asignar a un cargo, un proceso o grupo de trabajo que tendrá la responsabilidad de garantizar que la información y los activos asociados con los procesos se gestionen de manera adecuada.

10.1.3. Uso aceptable de Activos

Todos los funcionarios a los que se le haya asignado activos de información para el desarrollo de sus funciones contractuales, deben cumplir los siguientes lineamientos:

- Toda actividad de administración y operación que se realice con los activos de información de propiedad de EMPAS S.A, deben estar orientadas única y exclusivamente a cumplir con los procesos misionales de la Entidad.
- Todos los funcionarios deben aplicar los controles de seguridad definidos en el presente manual, para reducir riesgos que afecten la integridad, confidencialidad y disponibilidad de los activos de información.
- Los activos de información que almacenen o usen datos personales sensibles, tendrán acceso controlado que será garantizado por el responsable de la custodia de la información.
- Ningún funcionario puede compartir sus credenciales de autenticación para acceder a los activos de información.
- Cualquier modificación que se le deba hacer a los activos de información, debe ser autorizada por su propietario y verificada por el Área de Sistemas de Información.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 20 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- Todos los funcionarios deben reportar al Área de Sistemas de Información cualquier evento que pueda afectar la integridad, disponibilidad y confidencialidad de cualquier activo de información.
- Todos los funcionarios y/o contratistas serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.
- Es responsabilidad de todos los funcionarios y contratistas de EMPAS S.A. reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los activos de información.
- No está permitido el uso de los recursos tecnológicos para difundir o participar en actividades publicitarias externas a EMPAS S.A.

Uso Aceptable equipos de cómputo

- Cada equipo de cómputo, incluyendo computadoras de escritorio, laptops y periféricos, está asignado a un área funcional específica dentro de la empresa.
- Estos equipos deben permanecer en su ubicación designada, salvo que se requiera un traslado debidamente justificado y aprobado. Para traslados entre diferentes subgerencias, se deberá obtener autorización de la gerencia. En el caso de traslados dentro de la misma subgerencia, la aprobación deberá ser otorgada por el subgerente correspondiente.
- Los funcionarios son responsables de utilizar los equipos de cómputo exclusivamente en su área asignada.
- En caso de cambios de rol o traslado a otra área, el funcionario debe coordinar con el área de sistemas de información para asegurar la transferencia adecuada de la información laboral y correo electrónico, si es necesario.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 21 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- Una vez asignado los equipos, los funcionarios son responsables por todos los elementos que se encuentren incorporados (CPU, Teclado, Mouse, Pantalla, cargador, entre otros).
- La configuración, instalación, desinstalación y mantenimiento de hardware y software operativo, de aplicación y utilitario de los equipos de cómputo y de los dispositivos periféricos como impresoras o escáner, así como equipos de comunicaciones como Router, Switch y Access Point, son responsabilidad única del Área de Sistemas de Información de EMPAS S.A. o de la empresa contratada para realizar dicho mantenimiento.
- Los funcionarios tienen prohibido instalar cualquier tipo de software en los equipos de cómputo de la empresa.
- EMPAS S.A. E.S.P se reserva el derecho de acceso a todos los equipos usados para desempeñar los objetivos de la empresa, incluyendo cualquier dispositivo que procese, utilice, almacene o transmita información.
- No está permitido utilizar los recursos de la empresa para realizar otras tareas que no concuerden con la labor asignada.

Uso aceptable del correo corporativo

- Los funcionarios de EMPAS S.A. no deben emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos de la Entidad, en especial, cuentas de correo personal.
- Es responsabilidad del usuario que descarga información directamente de internet o a través del correo, revisar inmediatamente esta información por el antivirus que dispone la empresa antes de ser abierta y/o distribuida, así mismo como abstenerse de abrir correos de dudosa procedencia y/o asunto sospechoso; debido a que puede estar siendo víctima de ataques a través del correo electrónico.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 22 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- La responsabilidad del contenido de los mensajes de correo electrónico es del usuario remitente. En los procesos de reenvío de estos, no se deben alterar los datos originales.
- No está permitido crear, enviar, o retransmitir mensajes de correo electrónico que contengan contenido textual y/o gráfico que constituya acoso, que puedan contribuir a un ambiente de convivencia hostil, o que sean considerados difamatorios, explícitamente sexuales o que puedan ofender a alguien con base en su raza, género, nacionalidad, orientación sexual, religiosa o política, apariencia física, estrato social o discapacidad.
- Está prohibida la generación, reproducción y envío de mensajes en cadenas o similares, debido a que esto puede habilitar la propagación de código malicioso (virus, troyanos, entre otros), saturar el tráfico de correo causando indisponibilidad del servicio o provocar fuga de información a través de mecanismos como spam, phishing, entre otros.
- El envío de mensajes a grupos de usuarios como todos@empas.gov.co o contratistas@empas.gov.co únicamente está habilitado para la Gerencia, Subgerentes, jefes de Oficina, Asesores, Oficina de Comunicaciones y Prensa.
- Los mensajes de procedencia dudosa o desconocida no deben ser respondidos y deben ser clasificados por el usuario como correo no deseado. Lo anterior con el objeto de mitigar los riesgos relacionados con eventos de software malintencionado, en caso de que el usuario presente dudas con los correos recibidos deberá reportar al área de sistemas de información la cual se encargará de hacer una revisión segura de cada caso.
- Las diferentes áreas de la empresa cuentan con correos institucionales de forma genérica, como por ejemplo contabilidad@empas.gov.co, tesoreria@empas.gov.co, incapacidades@empas.gov.co, entre otros., dichos correos se recomiendan usar para las labores misionales del área y cuyo fin

		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 23 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

requiera la trazabilidad de correos enviados y recibidos a dicha área para los diferentes entes o empresas externas, lo que se busca con esta directriz es que se evite el uso de correos personales para comunicaciones que afecten al área en cuestión, y que ponga en riesgo el seguimiento de procesos o tareas críticas. (respuestas a entes de control, comunicaciones de novedades laborales, actuaciones y notificaciones legales, comunicaciones financieras y tributarias oficiales entre otros). En el caso de que un área necesite un correo adicional o no cuenta con este tipo de correo, debe solicitarlo al área de sistemas de información e indicar su redireccionamiento (si se llegase a requerir).

- El acceso a la consulta de los correos genéricos de las áreas, se hace a través del webmail (<http://mail.empas.gov.co/>) es responsabilidad del área encargada garantizar la custodia de los correos enviados y recibidos a través de dichas cuentas.



Figura 1: Portal de acceso webmail EMPAS

		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 24 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

10.2. CLASIFICACIÓN DE LA INFORMACIÓN

10.2.1. Clasificación de la Información

- Toda la información existente generada en EMPAS S.A. debe ser clasificada por su responsable, con el objetivo de determinar controles específicos para su protección. La metodología para la clasificación de la información está armonizada con la Ley 1712 de 2014 o Ley de Transparencia y su aplicación será liderada por el Área de Archivo.
- EMPAS S.A. dispone de un inventario de activos de información y un Índice de Información Clasificada y Reservada, actualizados con periodicidad anual de acuerdo a lo establecido en la ley 1712 de 2014 acerca de la Transparencia y Acceso a la Información Pública.

10.3. MANEJO DE MEDIOS

10.3.1. Gestión de Medios Removibles

- No está permitido el uso y conexión de dispositivos de almacenamiento (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, teléfonos móviles, etc.) sobre la infraestructura tecnológica de la empresa y únicamente se asignarán permisos a los funcionarios cuyo perfil del cargo y funciones lo requiera, previa solicitud a través del formato FOGI-04 con visto bueno del Asesor de Sistemas.
- Los usuarios que almacenen información confidencial o restringida de la empresa en el equipo de cómputo asignado, y que requieran realizar una copia de seguridad de la información para asegurar su disponibilidad deberá solicitar al área de soporte la realización de la misma, o realizarla de manera individual mediante los procedimientos y recursos aprobados por la empresa.
- Todo medio de almacenamiento removable debe ser sometido a análisis con la herramienta antivirus instalada en los equipos de EMPAS S.A.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 25 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- El Área de Sistemas de Información es responsable de implementar los controles necesarios para asegurar que únicamente los funcionarios autorizados, hagan uso de los medios removibles.
- Los medios de almacenamiento removibles que se conecten a los equipos de cómputo pueden estar sujetos a monitoreo por parte de Sistemas de Información, si se sospecha que incumplen las políticas descritas en este manual.
- EMPAS S.A. es consciente que este tipo de herramientas son muy útiles para el resguardo y transporte de información, pero igualmente son elementos que permiten extraer información sin dejar huella física ni registro de dicha acción; Por esta razón quien haga uso de estos medios con la debida autorización, debe velar por la integridad y privacidad de la información contenida.
- No está permitida la ejecución de programas no autorizados desde algún medio extraíble identificado anteriormente.
- Los medios de almacenamiento electrónico de datos y los medios físicos como el papel, que tengan información confidencial o restringida, deben ser físicamente destruidos antes de ser arrojados a la basura, los discos duros deben ser formateados. El papel impreso con información confidencial o restringida nunca debe ser reutilizado.

11. CONTROL DE ACCESO

11.1. REQUISITOS DE EMPAS PARA EL CONTROL DE ACCESO

Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y contraseña necesarios para acceder a la información y a la infraestructura tecnológica de EMPAS S.A, por lo cual deberá mantenerlo de forma confidencial e intransferible.

El permiso de acceso a la información que se encuentra en la infraestructura tecnológica de EMPAS S.A., debe ser proporcionado por el dueño de la información, con base en el principio de la “necesidad de saber” el cual establece que únicamente se deberán otorgar los permisos mínimos necesarios para el desempeño de sus funciones.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 26 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

11.1.1. Política de Control de Acceso Lógico

- Todos los usuarios y contratistas deben cumplir con la política de contraseñas.
- Cada funcionario es responsable del uso y protección de su usuario y contraseña para acceder a los recursos.
- Los usuarios deben autenticarse a través de los mecanismos de control de acceso proporcionados por el Área de Sistemas de Información antes de utilizar la infraestructura tecnológica, empleando contraseñas seguras.
- Está prohibido compartir información sobre los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica con personal externo.
- Los usuarios deben acceder únicamente a la información necesaria para realizar sus funciones laborales. El acceso a datos sensibles está restringido a quienes lo requieran por razones justificadas.
- Cada usuario debe tener una cuenta única, personal e intransferible, compuesta por las tres primeras letras de su nombre, las tres primeras letras de su apellido y el número "01". Si esta cuenta ya existe o coincide con la de otro usuario, se le asignará el siguiente número disponible.
- Los usuarios son responsables de todas las actividades realizadas con su cuenta de usuario.
- Los usuarios no deben divulgar ni permitir el uso de sus credenciales de acceso a los sistemas de información de la empresa por parte de terceros.
- Los equipos de cómputo deben estar configurados para bloquearse automáticamente tras un tiempo determinado, y este bloqueo debe estar protegido por la contraseña de inicio de sesión. Si algún usuario no tiene esta configuración o detecta que no funciona correctamente, deberá solicitar su revisión y/o configuración al área de soporte de Sistemas.
- El asesor del área de Gestión Humana notificará al correo de soporte ayuda@empas.gov.co y al asesor de gestión informática sobre el tiempo de

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 27 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

inactivación de la cuenta de acceso al dominio y del correo electrónico (según corresponda), en casos de encargos, vacaciones, finalización de la vinculación, incapacidades y licencias.

- El área de Sistemas asignará los roles y permisos necesarios al servidor público designado para asumir funciones mientras persista la situación que originó el control de acceso o cualquier otra novedad previa.
- En situaciones especiales, el asesor del área de Sistemas será responsable de asignar los tipos de restricciones correspondientes.
- Quien solicite un acceso a los sistemas de información de la empresa, deberá diligenciar los campos necesarios de manera digital del formato de registro de autorizaciones (FOGI-04).

11.1.2. Acceso a Redes y Servicios de Red

Intranet

La Intranet es un medio de comunicación interno y un sistema de gestión de la información que facilita el trabajo de las personas, por lo que es fundamental darle un uso adecuado. A través de la Intranet, se puede acceder a los distintos aplicativos institucionales utilizando el usuario y la contraseña asignados mediante el formato FOGI-04, previa solicitud. Esta contraseña es la misma que se utiliza para iniciar sesión en el dominio de trabajo.

Internet

- EMPAS S.A., con el objetivo de apoyar el desarrollo de las actividades institucionales, brinda acceso a Internet a sus funcionarios, con base en grupos de navegación definidos. Teniendo en cuenta que los recursos de la Entidad deben ser optimizados, los usuarios deben dar un uso racional al servicio de Internet y acoger los lineamientos de este Manual.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 28 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

El área de sistemas de información regulará la navegación por Internet con propósitos institucionales, educativos, de gobierno y demás páginas autorizadas por EMPAS S. A., de la siguiente manera:

- **Grupo Medio:** Este grupo tiene permitido la navegación a páginas institucionales, gubernamentales, educativas, portales de noticias, y otras páginas autorizadas que por el ejercicio de sus funciones requiera acceder. No tiene acceso a redes sociales, correo externo, YouTube, Dropbox o cualquier servicio de almacenamiento en la nube como cloud o drive online además no se permite ningún tipo de descarga.

Los usuarios incluidos en este grupo de navegación tendrán una 'hora feliz' de 7:30 a.m. a 8:30 a.m., durante la cual podrán acceder a correos externos (Hotmail, Gmail, Yahoo), YouTube y diversos periódicos, es decir, tendrán acceso completo a la navegación, con la excepción de redes sociales.

- **Grupo Alto:** Además de la navegación del grupo Medio, tendrá navegación completa incluye YouTube; y por definición no tiene acceso a las redes sociales.
- **Grupo Subgerentes:** Esta navegación incluye los dos grupos anteriores, más redes sociales, YouTube, restringiendo la descarga de archivos .exe o ejecutables.
- **Grupo Elite:** Este grupo será exclusivo para usuarios que deben realizar descargas de software, por lo tanto, el acceso es a todo nivel.

El Asesor de Gerencia de Sistemas será el encargado de autorizar con previa justificación del Asesor y Subgerente, o jefes de Oficina según corresponda el acceso en cualquiera de los grupos de navegación (alto, subgerentes) además del acceso a puertos USB y grabar CDs, para lo cual se requiere diligenciar el Formato de Registro de Autorizaciones - FOGI-04.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 29 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- No está permitido el uso y conexión de dispositivos alternos, que provean servicio a internet y/o configurar los dispositivos de la entidad para el acceso a estos medios alternos.
- No se permite utilizar software o servicios de mensajería instantánea (chat) y redes sociales no instalados o autorizados por Sistemas de Información.
- La entidad se reserva el derecho de realizar revisiones periódicas al cumplimiento de los lineamientos definidos sobre el uso de Internet. y podrá aplicar restricciones o medidas en caso de que se encuentren excesos o la utilización indebida de ese recurso.
- No está permitido el acceso a sitios pornográficos, con especial énfasis en los que involucran pornografía infantil, de contenido erótico, obsceno y sitios terroristas.
- Los usuarios que utilicen Internet institucional para la realización de transacciones comerciales de carácter personal como pago de facturas, transacciones bancarias, entre otras, deben asumir los riesgos que dichas transacciones implican. EMPAS S.A. no se hace responsable de la seguridad de las mismas, incluyendo la información que se transmita y que pueda ser objeto del monitoreo que se realiza al uso de Internet.
- La utilización de chat o mensajería instantánea, radio o video streaming es discrecional (usando audífonos o diademas para respetar los espacios personales) y está sujeta a la definición de perfiles de navegación que realice el área de sistemas de información. El acceso a sitios web que no se encuentren dentro de las categorías mencionadas en el MAGI-01, pero que requieran ser accedidas por los funcionarios para cumplir con sus obligaciones, podrán ser autorizados previa solicitud del jefe de área.
- Dado que la Entidad tiene la obligación legal de utilizar software licenciado, y que está comprometida con la protección de los derechos de propiedad

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 30 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

intelectual y de autor además de la optimización del recurso de ancho de banda de las redes, los usuarios no deben descargar desde Internet, almacenar en la plataforma tecnológica de EMPAS S.A. y/o usar software, música, libros, publicaciones, video y cualquier otro material protegido por derechos de autor, sobre el cual la Entidad no haya realizado el pago de los derechos patrimoniales que corresponda.

- EMPAS S.A., con el objeto de dar cumplimiento a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones a través de la Política de Gobierno Digital, dispone de cuentas en redes sociales, que se encuentran formalmente asignadas a unos responsables, por parte de la Oficina Asesora de Comunicaciones y que deben ser utilizadas bajo los protocolos de uso institucional, definidos para tal fin.
- Queda prohibido y se considerará como una falta grave:
 - 1) Acceso no autorizado a sitios web restringidos: Ingresar a sitios prohibidos por la empresa, como páginas de contenido explícito, ilegales o que comprometan la seguridad de la organización.
 - 2) Uso indebido de redes sociales: Utilizar redes sociales para compartir información confidencial, publicar comentarios ofensivos o comprometer la imagen de la empresa.
 - 3) Descarga de software no autorizado: Descargar, instalar o ejecutar software no autorizado que pueda comprometer la seguridad de la red o violar las políticas de propiedad intelectual.
 - 4) Uso excesivo de internet para fines personales: Navegar en internet para asuntos personales durante horas de trabajo, afectando la productividad y el rendimiento laboral.
 - 5) Acceso y difusión de material inapropiado: Compartir o acceder a material ofensivo, violento, discriminatorio o que vaya en contra de los valores de la empresa, ya sea a través del correo electrónico o de internet.
 - 6) Manipulación o elusión de políticas de seguridad: Intentar deshabilitar o evitar los controles de seguridad implementados para regular el acceso a internet y redes sociales.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 31 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

7) Uso de internet para actividades ilícitas: Emplear la red de la empresa para actividades ilegales, como piratería, fraudes, acoso o violaciones a derechos de propiedad intelectual.

8) Acceso no autorizado a sistemas o datos internos: Intentar acceder o distribuir información sensible o confidencial sin autorización, tanto dentro como fuera de la empresa.

9) Uso indebido de la infraestructura tecnológica: Utilizar los recursos de la empresa, como el correo electrónico o el internet, para fines comerciales personales o ajenos a la misión de la empresa.

10) Suplantación o uso no autorizado de cuentas: Acceder a internet o sistemas de información utilizando cuentas de otros empleados sin su autorización, comprometiendo la seguridad y privacidad de la información.

11) Toda conexión remota desde el exterior de EMPAS S.A que no haya sido autorizada por el nivel directivo con observancia a los niveles de control respectivo, con la salvedad de los servicios corporativos que sean habilitados para su uso remoto. Esta autorización sólo se concederá cuando la función asignada al cargo lo requiera, y tras tener garantías suficientes de que no se verán afectados los niveles de seguridad de los sistemas de Información de la empresa.

Carpetas compartidas

El acceso a carpetas compartidas debe ser concedido únicamente a empleados que lo requieran para cumplir con sus responsabilidades laborales. Las solicitudes de acceso deben pasar por un proceso formal de autorización, aprobado por el supervisor, dueño de la información compartida y del área de sistemas de información.

Los permisos deben ser específicos, limitando el acceso solo a las carpetas que el usuario necesite y con los niveles de acceso de acuerdo a las necesidades (lectura o lectura y escritura). (Ver instructivo ITGI-05 para el uso de las carpetas compartidas),

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 32 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

Se debe clasificar la información dentro de las carpetas compartidas por niveles de sensibilidad (pública - interna). El acceso debe otorgarse de acuerdo con estos niveles, en ningún momento se tiene autorización de compartir información sensible, confidencial o crítica para estas se debe hacer uso de la NUBE EMPAS (Ver instructivo ITGI-04 para utilizar la Nube en EMPAS) la cual deberá solicitarse al Área de Sistemas de Información previa autorización del asesor o jefe inmediato, esto con el fin de prevenir la proliferación de virus informáticos en los equipos de cómputo de la institución y reducir el riesgo de compartir información sensible.

Los usuarios deben asegurarse de que la información contenida en las carpetas compartidas esté protegida y que se realicen copias de seguridad de manera regular para evitar la pérdida de datos, el área de sistemas de información no se hace responsable de la pérdida o daño de información contenida en estos medios en caso que se requiera que haya una mayor gestión sobre la información se debe solicitar de manera formal la creación de un espacio en el servidor de archivos, así mismo se deben establecer políticas de retención de archivos y eliminación segura de documentos antiguos o innecesarios para evitar la acumulación de información obsoleta o comprometida, también es importante que los usuarios conozcan que no está permitido almacenar información personal o no relacionada con el trabajo en carpetas compartidas.

Cuando el acceso a carpetas compartidas sea necesario de manera temporal (por ejemplo, para contratistas o empleados que colaboren en proyectos específicos), debe tener una fecha de expiración clara y debe ser revocado inmediatamente después de completado el proyecto o la tarea, para lo cual se debe informar las fechas correspondientes a la ejecución del proyecto.

11.2. GESTIÓN DE ACCESO DE USUARIOS

- Los ingenieros de soporte adscritos al área de Sistemas de Información junto con los responsables de las aplicaciones deben revisar los derechos de acceso de los usuarios por lo menos una vez al año.
- El acceso a las plataformas, aplicaciones, servicios y, en general, a cualquier recurso de información de EMPAS S.A. debe contar con la autorización de las

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 33 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

dependencias propietarias de los sistemas de información que contenga información sensible o datos personales, debe venir acompañado con el diligenciamiento del formato - FOGI-04 formato registro de autorizaciones,

- Siguiendo el principio de mínimo privilegio se deberá otorgar a los usuarios únicamente los permisos necesarios para realizar sus tareas laborales, garantizando que los permisos se otorguen de acuerdo con el rol del usuario en la organización. Esto asegura una gestión más eficiente y controlada de los accesos.
- No está permitido divulgar, compartir, distribuir, asignar, permitir, entregar, alquilar, comunicar, intercambiar, vender y/o prestar la contraseña de él(los) usuario(s) administrador(es) de la plataforma tecnología, dispositivos, bases de datos, equipos, servidores, aplicaciones, sistemas de información y similares.
- Toda asignación de permisos de acceso privilegiado debe contar con previa autorización del área de sistemas.
- Los derechos de acceso de todos los funcionarios, contratistas y terceros de acceso a la información y a los servicios de procesamiento de información se deben retirar al terminar su contratación laboral, contrato o acuerdo y/o se deben ajustar cuando existan cambios de dependencias y/o responsabilidades.
- El área de Gestión Humana debe informar al Área de Sistemas de Información, retiros, traslados o nuevos roles del personal adscrito a la Empresa, puesto que es primordial tener actualizada la base de datos del sistema de atención al usuario, cuentas de correo y equipos de cómputo. Además, que el área de sistemas es la responsable de adelantar el proceso formal para desactivar o modificar los accesos de los usuarios que abandonen la empresa o cambien de puesto.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 34 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

11.2.1. Administración de Privilegios

Cualquier cambio en los roles y responsabilidades de los usuarios en los Aplicativos deberán ser notificados al Área de Sistemas de Información, a excepción de los aplicativos netamente técnicos contratados y administrados por otra Área.

11.2.2. Equipo Desatendido

- Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente instalados y autorizados por el Área de Sistemas de Información cuando no se encuentren en su lugar de trabajo.
- Los empleados de planta y contratistas deben asegurarse en el momento en que dejen su puesto de trabajo u oficina, que sus computadores estén apagados o bloqueados.
- El área de Sistemas de Información asegurará la implementación del bloqueo automático de pantalla mediante una política de dominio establecida por el asesor del área.

11.2.3. Políticas de Uso de Dispositivos de Almacenamientos Externos

Está restringido el uso de dispositivos de almacenamiento externo como:

- a. Memoria Flash USB
- b. Reproductores portátiles MP3/MP4
- c. Cámaras con conexión USB
- d. Smartphones
- e. SD Cards/Mini SD Cards/Micro SD Cards.
- f. PDAS/Tablets
- g. Dispositivos con tecnología Bluetooth
- h. Tarjetas Compact Flash
- i. Discos duros de uso externo
- j. Cualquier otro medio de almacenamiento externo

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 35 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

11.3. RESPONSABILIDAD DE LOS USUARIOS

Todos los funcionarios y contratistas, cuentan con un usuario y contraseña única, personal e intransferible y asumen la responsabilidad de los eventos e incidentes que puedan ocurrir bajo el uso de los mismos como mecanismo de autenticación sobre los activos de información a los cuales acceden y procesan dentro del desarrollo de sus funciones.

Se deben tener en cuenta las siguientes recomendaciones para el manejo y buen uso de las contraseñas:

- Los funcionarios y contratistas, que requieran tener acceso a los equipos de cómputo y/o sistemas de información de EMPAS S.A. deben tener contraseñas con un alto grado de seguridad, por lo tanto, deben incluir: Una longitud mínima de 10 caracteres, alfanumérica, al menos una letra mayúscula y uno o más caracteres especiales (como \$! % & *).
- Cuando un usuario olvide o bloquee su contraseña, deberá acudir al Área de Sistemas de Información para que se le proporcione una nueva o restablezca.
- Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.
- Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con la misma.
- Todo usuario que sospeche que su contraseña es conocida por otra persona, deberá por precaución cambiarla inmediatamente.
- El usuario deberá cambiar la contraseña inicial que se le asigne, en el primer acceso que realice al Sistema.
- Se recomienda no incluir en la contraseña palabras, fechas (cumpleaños) o términos relacionados directamente con el empleado.
- No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.

		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 36 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- Las contraseñas deben ser actualizadas por los usuarios cada vez que lo consideren necesario utilizando CTRL + ALT + SUPR, opción cambiar una contraseña y como mínimo una vez cada tres meses.
- Es obligatorio cambiar la contraseña cada 90 días, de lo contrario, esta caducará y automáticamente el usuario no podrá ingresar al equipo.
- No se permite repetir ninguna de las últimas 5 contraseñas usadas anteriormente ya que el sistema las detectará y no permitirá el inicio de sesión.
- Tras 6 intentos fallidos de ingresar la contraseña por parte del usuario esta se bloqueará por 5 minutos y pasado ese tiempo podrá intentar nuevamente el proceso de ingreso de la misma.
- Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

Se debe dar uso adecuado a los activos de información y deben ser usados únicamente bajo los términos y condiciones laborales.

La Gerencia General, la Subgerencia Administrativa y Financiera y el Área de Sistemas de Información, podrán bloquear el acceso si se sospecha que existe un riesgo.

11.4. CONTROL DE ACCESO A LOS SISTEMAS Y APLICATIVOS

El Área de Sistemas de Información es la única dependencia autorizada para crear, asignar, bloquear, retirar y modificar usuarios y permisos de acceso a los sistemas de la empresa.

Control de datos en las aplicaciones

El Área de Sistemas de Información, implementará controles para garantizar que los datos de entrada y salida del sistema sean verificables en términos de integridad, exactitud y validez.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 37 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

Restringirá los datos de salida de las aplicaciones de la empresa mediante controles lógicos, de acuerdo con los permisos de acceso establecidos.

Establecerá medidas de identificación y autenticación para el acceso a dichos datos.

12. SEGURIDAD FISICA Y DEL ENTORNO

Los mecanismos de control de acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y Áreas restringidas de la EMPRESA sólo a personas autorizadas para salvaguardar los equipos de cómputo y comunicaciones de la empresa.

12.1. ÁREAS SEGURAS

- Cuando los usuarios se ausenten de sus estaciones de trabajo deberán cerrar todas las aplicaciones y documentos propios de su actividad a fin de prevenir que sus documentos o soportes de información sean sustraídos con facilidad, o que sean modificados o eliminados, así mismo deberán apagar íntegramente el equipo, incluyendo pantalla y CPU en cumplimiento a las medidas ambientales y de austeridad en el gasto.
- Se restringe el acceso físico a las áreas críticas (cuartos de servidores) a usuarios no permitidos y a fin de controlar y minimizar el riesgo de accidentes y actividades fraudulentas. Solo tiene permitido el acceso, al personal del Área de Sistemas de Información. el ingreso de otro personal para actividades asociadas a los mantenimientos de Aires acondicionados, UPS, Verificación de inventarios, Arreglos locativos, etc., será autorizado por el área de Servicios Generales. Posteriormente los funcionarios de Sistemas de Información verificarán el estado del Centro de Procesamiento de Datos con el fin de evidenciar si se presentó algún daño o alteraciones en los Equipos.
- El Área de Servicios Generales dispone de una copia de las llaves de cada cuarto técnico de servidores, tanto de la sede administrativa como de la sede de alcantarillado. Estas llaves se entregan al personal de vigilancia con el propósito de garantizar el funcionamiento adecuado de los aires acondicionados. En caso de una falla en el sistema eléctrico durante horarios nocturnos o fines de semana, el personal de vigilancia está autorizado a abrir puertas y ventanas para permitir

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 38 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

la ventilación y evitar el sobrecalentamiento en el área. Una vez restablecido el suministro eléctrico, deberán encender los aires acondicionados y asegurarse de cerrar nuevamente el área.

- Se deberán utilizar sistemas de monitoreo automáticos o manuales, que controlen el acceso constantemente.

12.2. EQUIPOS

- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos. En caso de requerir este servicio deberá solicitarlo al Área de Sistemas de Información.
- Está prohibido conectar a la red interna de EMPAS equipos de cómputo personales para las labores desempeñadas en la empresa, salvo autorización por parte del asesor de gerencia de sistemas de información, y verificando la legalidad del software instalado en dicho equipo por parte del área de sistemas.
- La instalación, traslado y configuración de computadores, elementos de red, servidores, periféricos y en general cualquier equipo de cómputo que se integre a la red corporativa de la empresa será realizado únicamente por personal del Área de Sistemas de Información, previa autorización del Directivo Responsable de cada Proceso.
- El Área de Sistemas de Información será la única encargada de llevar a cabo el encendido y apagado de los servidores que se utilizan en EMPAS S.A., siguiendo el instructivo para desarrollar esta actividad. (ITGI-02).
- El cableado de la energía y las telecomunicaciones que llevan datos o sostienen los servicios de información deben permanecer protegidos a través de canaleta para evitar el deterioro y garantizar la disponibilidad del servicio.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 39 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Los Usuarios deben evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU y mantener el equipo informático en un entorno limpio y sin humedad.
- Todos los equipos que contengan información sensible y/o confidencial en sus medios de almacenamiento deben pasar por un procedimiento de borrado seguro antes de su reutilización o finalización de su vida útil.
- El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos.
- Está prohibido que el usuario destape o desarme los equipos de cómputo.
- Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica de EMPAS S.A, deberán ser solicitados al Área de Sistemas de Información.
- Los equipos de cómputo de la empresa deberán tener una contraseña de administrador para la configuración del sistema operativo, que deberá gestionar el administrador de la red.
- Se prohíbe extraer de su ubicación cualquier elemento hardware, excepto aquellos que por su característica de portátil o móvil sean dedicados a aplicaciones de movilidad, tales como los computadores Portátiles.
- El usuario será responsable de salvaguardar su información almacenada en su equipo.

		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 40 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- Los usuarios no podrán modificar las medidas técnicas de seguridad implantadas en los equipos de cómputo.
- Únicamente el personal autorizado por el Asesor de Gerencia - Sistemas de Información podrá llevar a cabo los servicios y reparaciones al equipo informático.
- El usuario deberá dar aviso inmediato al Área de Sistemas de Información y Servicios Generales de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su custodia para su reposición, investigación y acciones administrativas y disciplinarias a lugar.
- En el supuesto de que se produjera cualquier situación que pudiera poner en riesgo la seguridad de los sistemas de información de la empresa, el usuario deberá notificar la incidencia producida inmediatamente al Área de Sistemas de Información
- Los Usuarios deben velar por utilizar en forma debida las instalaciones eléctricas reguladas (ejemplo: REG.-1 – UPS2) garantizando la continuidad del encendido en los equipos una vez sea interrumpido el fluido eléctrico, y abstenerse de conectar a ella equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que sobrecargue los puntos, esto puede generar caídas de energía e incluso inconvenientes de mayor magnitud a la plataforma.
- La Empresa debe suministrar los siguientes dispositivos de seguridad y soporte que garantizan la continuidad de los equipos:
 - a. Aire acondicionado
 - b. Extintores
 - c. UPS (Uninterruptible Power Supply)
 - d. Descarga a tierra

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 41 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- Todos estos dispositivos de seguridad serán evaluados por personal de mantenimiento encargado por parte de la Subgerencia Administrativa y Financiera.
- Como elemento de control se utilizará un tablero de distribución con sus respectivos interruptores de energía en la salida de emergencias de cada edificio.

13. SEGURIDAD DE LAS OPERACIONES

13.1. PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES

Es responsabilidad del Área de Sistemas de Información separar los ambientes de desarrollo, pruebas y producción de los desarrollos internos y externos.

13.2. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

- En todos los equipos de la empresa debe existir una herramienta antivirus ejecutándose permanentemente, para lo cual existe un procedimiento para la instalación y actualización del antivirus (ver anexo técnico)
- Se prohíbe compartir en su totalidad el disco duro. De ser necesario compartir información, se debe crear una carpeta compartida en la cual se puede almacenar la información que es considerada temporal (Ver instructivo ITGI-05 para el uso de las carpetas compartidas) o hacer uso de la NUBE EMPAS (Ver instructivo ITGI-04 para utilizar la Nube en EMPAS) la cual deberá solicitarse al Área de Sistemas de Información previa autorización del Subgerente de cada dependencia, esto con el fin de prevenir la proliferación de virus informáticos en los Equipos de Cómputo de la institución.
- La entidad cuenta con un FIREWALL (dispositivo que funciona como cortafuegos, permitiendo o denegando las transmisiones de una red a otra). El firewall de la empresa debe configurarse de manera que se prohíban todos los

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 42 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

protocolos y servicios que pongan en riesgo la seguridad de la información, habilitando los estrictamente necesarios.

- Los usuarios de EMPAS S.A que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser spam, phishing, espías, virus, caballos de Troya, gusanos de red entre otros.
- Toda solicitud de instalación de software debidamente licenciado que no sea propiedad de EMPAS S.A, deberán justificar su uso y legalidad ante el Área de Sistemas de Información, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá este software.
- Se considera una falta grave que los usuarios instalen cualquier tipo de programa (software) en sus computadores, estaciones de trabajo, servidores, o cualquier equipo conectado a la red de EMPAS S.A, que no esté autorizado por el Área de Sistemas de Información.
- Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de los Directivos competentes, el usuario informático deberá notificar esta situación al Subgerente respectivo.
- Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el Área de Sistemas de Información, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de EMPAS S.A, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.
- Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 43 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa a EMPAS S.A, a menos que cuente con la autorización del Directivo correspondiente.

- EMPAS S.A se reserva el derecho a acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal que ha comprometido la seguridad, violado políticas de Seguridad Informática de esta Empresa o realizado acciones no autorizadas.
- El usuario debe tener claro que el correo electrónico de EMPAS S.A. es un correo de trabajo y No Personal, y se debe utilizar única y exclusivamente a los recursos que tenga asignados y las facultades que se le concedieron, para el desempeño de su empleo, cargo o comisión quedando prohibido cualquier otro uso.
- Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.
- Los usuarios autorizados para el manejo de discos flexibles, CD's, DVD's, discos externos y USB, deben tener la cultura de verificar que la información y estos medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el Área de Sistemas de Información.
- Todos los archivos de computador que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 44 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- Ningún usuario de EMPAS S.A debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computador diseñado para auto replicarse, dañar, o en otros casos impedir el funcionamiento de cualquier memoria de computador, archivos de sistema, o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas de EMPAS S.A. El incumplimiento de este estándar será considerado una falta grave, debido a que estaría atentando contra la plataforma y red de nuestra entidad.
- Cualquier usuario que sospeche de alguna infección por virus de computador, deberá dejar de usar inmediatamente el equipo y comunicar al Área de Sistemas de Información para la detección y erradicación del virus.
- Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por EMPAS S.A en: Antivirus, Outlook, Office, Navegadores u otros programas.

13.3. COPIAS DE RESPALDO

- El Área de Sistemas de Información realizará copias de seguridad periódicas atendiendo a la criticidad de la información y se establecerá y cumplirá la política de realización de backups de acuerdo al plan de copias de seguridad de la Información.
- Para los sistemas de información que son gestionados y administrados por Dependencias del área técnica, es necesario que estas envíen comunicación formal al Asesor de Gerencia de Sistemas de Información con el fin de indicar cuales archivos se deben salvaguardar y su frecuencia de copiado. Cuando se requiera el acceso a un Backup deberá solicitarlo formalmente al Área de Sistemas. Cada vez que se produzca algún cambio deberá notificarse a Sistemas de Información para la reprogramación de la copia respectiva.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 45 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- En caso de requerirse la inclusión de información adicional en el Plan de Copias de Seguridad, el jefe de área debe solicitarlo por escrito al área de sistemas de información.
- El Área de Sistemas de información es la encargada de verificar que las copias se generen de manera correcta y de la restauración de los Backups, las copias manuales realizadas serán registradas en el formato FOGI-03 – Formato de registro de copias de seguridad y serán revisadas por el asesor de gerencia de sistemas de información
- Si el funcionario considera que se debe realizar una copia de la información contenida en su equipo de cómputo, esta debe ser solicitada a través de un correo electrónico (ayuda@empas.gov.co) al área de sistemas, especificando la ruta y los archivos donde se encuentra dicha información.
- En el Plan de Contingencia Tecnológica PLGI-01 están definidos los lineamientos correspondientes a los procedimientos de recuperación y respaldo de las copias.

13.4. REGISTRO Y SEGUIMIENTO

- Se debe conservar un registro de todos los códigos fuente y las librerías de los aplicativos propiedad de EMPAS S.A. con el fin de facilitar las labores de revisión.
- Todos los relojes de los sistemas de procesamiento de información de EMPAS S.A. deben estar sincronizados con una fuente de tiempo exacto acordado.
- Seguridad de Bases de Datos

Los archivos indexados de la empresa, las carpetas donde se encuentran almacenados y las aplicaciones que los administran deberán tener controles de acceso, de forma tal que la única persona que pueda tener acceso a estos recursos sea el administrador de las Bases de Datos. Deberán hacerse chequeos regulares de la seguridad de la base de datos, para verificar que:

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 46 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- a. Se hacen y son efectivos los Backups y los mecanismos de seguridad
- b. No haya usuarios de la base de datos que no tengan asignado una contraseña
- c. Se revisen los perfiles de los usuarios que no han usado la base de datos por un período largo de tiempo.
- d. Nadie, además del administrador de datos, ha accedido a los archivos del software de base de datos y ha ejecutado un editor de archivos indexados.
- e. Solo el administrador de datos tiene acceso de lectura y escritura en los archivos de programa.
- f. La base de datos y las aplicaciones que la administran tiene suficientes recursos libres para trabajar eficientemente.
- g. Deben mantenerse registros de todas las transacciones realizadas en la base de datos, de manera que éstas puedan revertirse en caso de surgir un problema.
- h. Los registros de la base de datos no se borrarán físicamente, sino que deberán marcarse como eliminados.

13.5. CONTROL DE SOFTWARE OPERACIONAL

- La instalación de cualquier tipo de software en la empresa es función y responsabilidad exclusiva del Área de Sistemas de Información; cualquier otro software instalado sin autorización será responsabilidad del usuario.
- En caso de la detección de la instalación de un software sin el cumplimiento normativo, el Área de Sistemas de Información de manera inmediata procederá a desinstalar y reportar esta situación al jefe inmediato.

		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 47 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- El Área de Sistemas de Información será la encargada de implementar las mejoras solicitadas por los usuarios y los ajustes de las características que se definan en el área a los sistemas de información en producción.
- Para la parametrización, alimentación y validación de las aplicaciones es necesario contar con el apoyo de los usuarios del sistema de información, esto solo para los Aplicativos que gestiona Sistemas de Información.
- Cada responsable de cada proceso solicitará ante la Gerencia la necesidad de compra o implementación de nuevos programas para el desarrollo de sus actividades especificando sus requerimientos.
- El Área de Sistemas de Información, evaluará la viabilidad de adquirir nuevos sistemas o aplicativos previa solicitud de las dependencias y dará su concepto técnico para la toma oportuna de su decisión en caso de ser requerido por la Gerencia General y/o Subgerencias.
- El grupo de soporte a usuarios adelantarán periódicamente revisiones para verificar el estado de licenciamiento de software de cada equipo al servicio de la empresa, demostrando que el software es gratuito o licenciado y que su uso es indispensable para el cumplimiento de sus funciones.
- Los accesos o perfiles de los usuarios tendrán la vigencia que se determine en el diligenciamiento del FOGI-04 formato registro de autorizaciones. Para el caso de personal de planta y una vez finalice su relación laboral con la empresa, se debe diligenciar el FOGF-06 formato paz y salvo, inmediatamente firmado se procede a la cancelación de la cuenta de red y correo electrónico.

13.6. GESTIÓN DE LA VULNERABILIDAD TÉCNICA

- Se deben realizar análisis de vulnerabilidades y riesgos para actualizar la matriz de riesgos del proceso de Gestión Informática.
- No está permitido que los funcionarios, contratistas y terceros realicen pruebas y/o aprovechen las debilidades de seguridad en la infraestructura tecnológica.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 48 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

- Se debe restringir la práctica de instalación de software no autorizado a través de políticas de dominio y otorgar los permisos únicamente a los funcionarios autorizados.

14. SEGURIDAD DE LAS COMUNICACIONES

14.1. GESTIÓN DE LA SEGURIDAD DE LAS REDES

Algunos sistemas de información tienen interoperabilidad y a través de la Red Interna de la Empresa y con terceros fuera de ella, por lo tanto, es necesario establecer criterios de seguridad en las comunicaciones.

La empresa cuenta con un plan de contingencia tecnológico, que contiene los lineamientos y metodologías necesarias para poder continuar con las operaciones, procesos y servicios informáticos críticos, en caso de que se llegara a presentar algún siniestro o contingencia. Así como minimizar el impacto que dichos daños pudieran causar el cual se puede consultar por el área de sistemas de información.

14.1.1. Topología de Red

El Área de Sistemas de Información deberá asegurar la integridad, disponibilidad y confidencialidad de los datos transmitidos, ya sea a través de dispositivos de hardware, de los protocolos de transmisión, o de los controles de aplicativos.

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la Entidad, deberán ser consideradas y tratadas como información confidencial.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 49 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

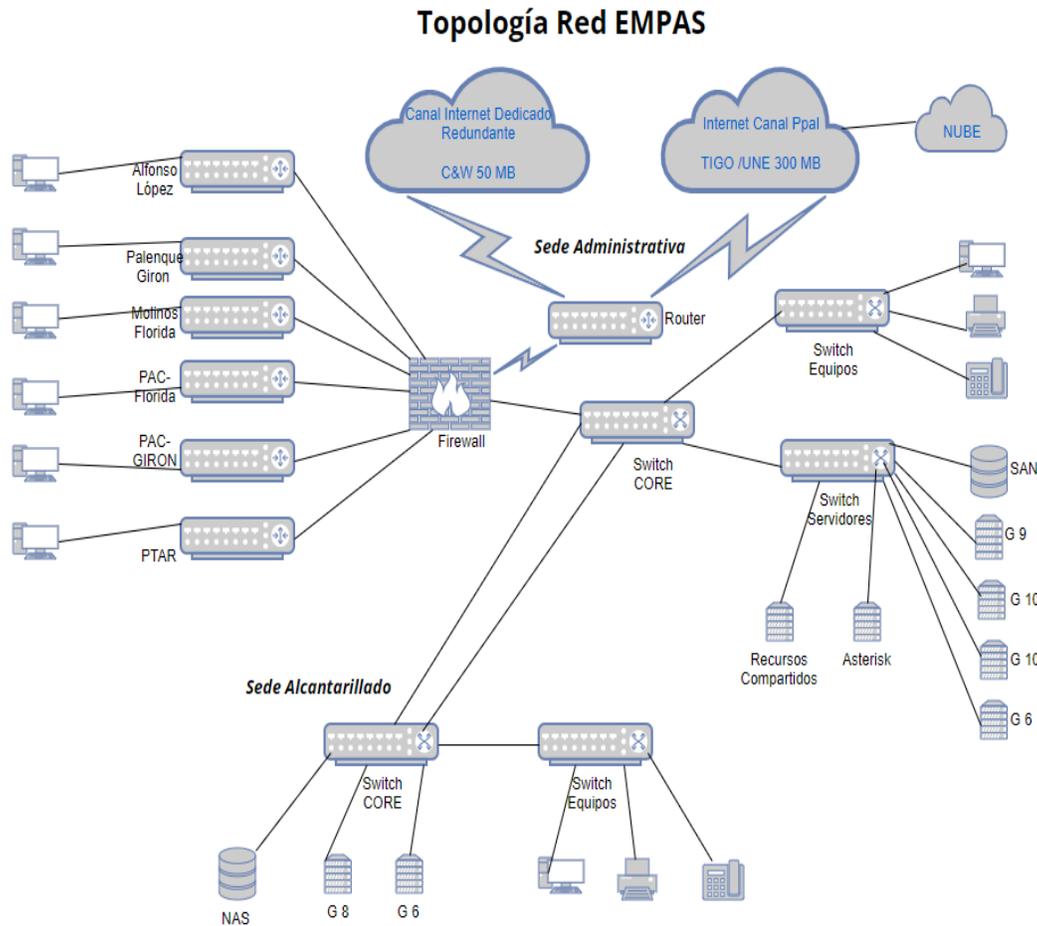


Figura 2. Topología de Red EMPAS S.A

14.1.2. Conexiones Externas

El Área de Sistemas de Información deberá asegurar la implementación de elementos de control en las actividades de conexiones externas de EMPAS S.A a fin de garantizar la adecuada protección de los bienes de información de la organización. Remítase a la sección de trabajo en casa y acceso remoto.

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 50 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

14.2. TRANSFERENCIA DE INFORMACION

El intercambio de información entre empleados, contratistas y las diferentes áreas por medio electrónico debe ser realizado a través de correo institucional, carpeta compartida o nube privada de la empresa.

Si la transferencia es a través del correo institucional la información enviada deberá incluir la respectiva firma del remitente y en su pie de página el siguiente aviso:

“LA EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P – EMPAS S.A. dando cumplimiento a lo estipulado en la Ley 1581 de 2012 y su decreto reglamentario 1074 de 2015, tendiente a la protección de datos personales lo invita a que conozca la Política de Tratamiento de Datos Personales la cual puede ser consultada en las instalaciones físicas de la entidad o en el sitio web www.empas.gov.co. En dicha política se establecen los derechos que le asisten como titular, el procedimiento para ejercerlos, las finalidades para la cual se tratan los datos, entre otros aspectos. Si usted tiene alguna inquietud frente al manejo de la información, envíe su solicitud a través de nuestra página web o al correo contactenos@empas.gov.co y con gusto será atendido.”

15. REFERENCIAS

- Guía 8 - Controles de Seguridad de la Información MINTIC.
- NTC-ISO/IEC 27001.
- NTC-ISO/IEC 27002.
- Modelo Integrado de Planeación y Gestión, MIPG.
- Estrategia de uso y apropiación de TI.
- Plan de contingencia tecnológico

 EMPAS <small>EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.</small>		EMPRESA PÚBLICA DE ALCANTARILLADO DE SANTANDER S.A. E.S.P.		
CÓDIGO: MAGI-01-04	FECHA: 27/11/2024	ELABORÓ: ÁREA SISTEMAS DE INFORMACIÓN	REVISÓ: ASESORA DE GERENCIA- PLANEACIÓN CORPORATIVA Y CALIDAD	APROBÓ: COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO
CONTROL: SI	PÁGINA: Pág. 51 de 51	MANUAL DE ADMINISTRACIÓN DE TECNOLOGÍAS, SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE EMPAS S.A.		

ANEXOS

ANEXO 1. PROCEDIMIENTO DE GENERACIÓN Y RESTAURACIÓN DE COPIAS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

Este documento es relacionado con fines exclusivamente informativos y no será publicado ya que el contenido del mismo es de confidencialidad e importancia para el Área de Sistemas de Información.

ANEXO 2. PROCEDIMIENTO PARA LA INSTALACIÓN Y ACTUALIZACIÓN DEL ANTIVIRUS.

Este documento es relacionado con fines exclusivamente informativos y no será publicado ya que el contenido del mismo es de confidencialidad e importancia para el Área de Sistemas de Información.